Deployment Guide

AX Series with Microsoft Windows Server 2008 Terminal Services

Version: 1.1

Table of Contents

DEPLOYMENT GUIDE

AX Series with Microsoft Windows Server 2008 Terminal Services

Introduction

This deployment guide contains configuration procedures for AX Series application delivery controllers and server load balancers to support Windows Server 2008 Terminal Services.

Microsoft Terminal Services (TS) allows users to remotely control the whole desktop or certain applications. Microsoft provides three TS access modes:

- Remote Desktop Connection (RDC)
- Remote Desktop Connection with TS Gateway (RDC with TSGW)
- Web Access

For more information on Microsoft TS 2008, visit:

http://www.microsoft.com/Windowsserver2008/en/us/ts-product-home.aspx

The AX Series with its Advanced Core Operating System (ACOS) has been designed specifically for applications such as TS, providing more robust response in failover situations, offloading security processing, and performing intelligent load sharing for all three TS access modes.

Prerequisites & Assumptions

- A10 Networks' AX platform should be running software version 2.0 or later.
- It is assumed that users have some basic configuration familiarity with both AX and Microsoft TS products.
- The AX can be configured in one-armed mode or routed mode.
- Microsoft screenshots are from Windows 2008R2 TS servers.
- Note: A10 supports Microsoft 2008 and Windows 2003 TS servers too. The same A10 configuration can be applied for them.
- Both IPv4 and IPv6 Windows TS are supported. The examples in this deployment guides use IPv4.

AX deployment for Windows TS with RDC access

Windows 2008 enhanced TS with a new role: Session Broker. TS Session Broker provides simple load balancing and user persistency to the TS Server.

Microsoft recommends Session Broker for Terminal Server farms of two to five servers. (http://download.microsoft.com/download/b/b/5/bb50037f-e4ae-40d1-a898-7cdfcf0ee9d8/All-Up/WS08AndWS03ComparisonFinal_En.docx.)

AX fully supports Microsoft TS and allows:

- Large TS farms
- Granular TS load balancing and availability options
- TS in private networks (not directly reachable from outside)

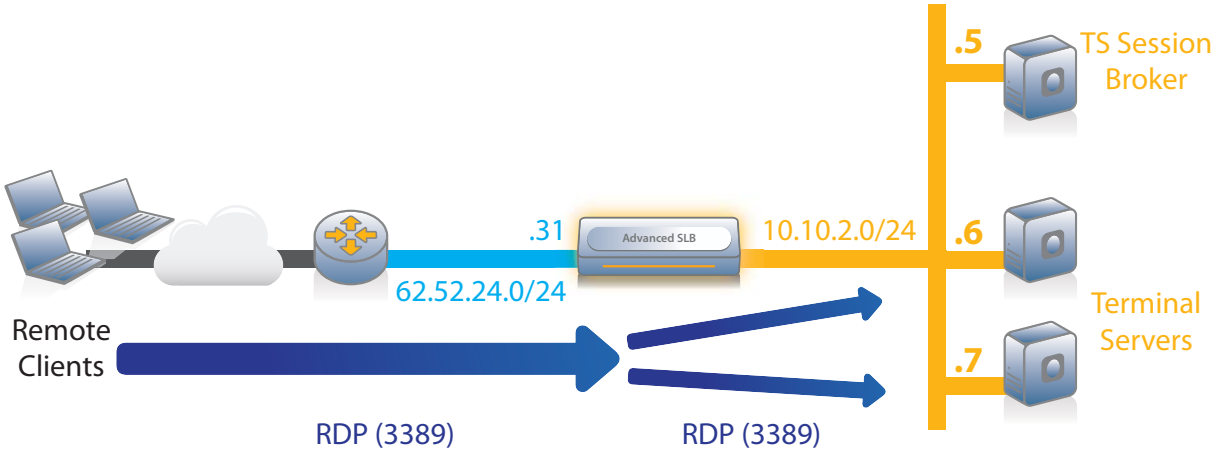


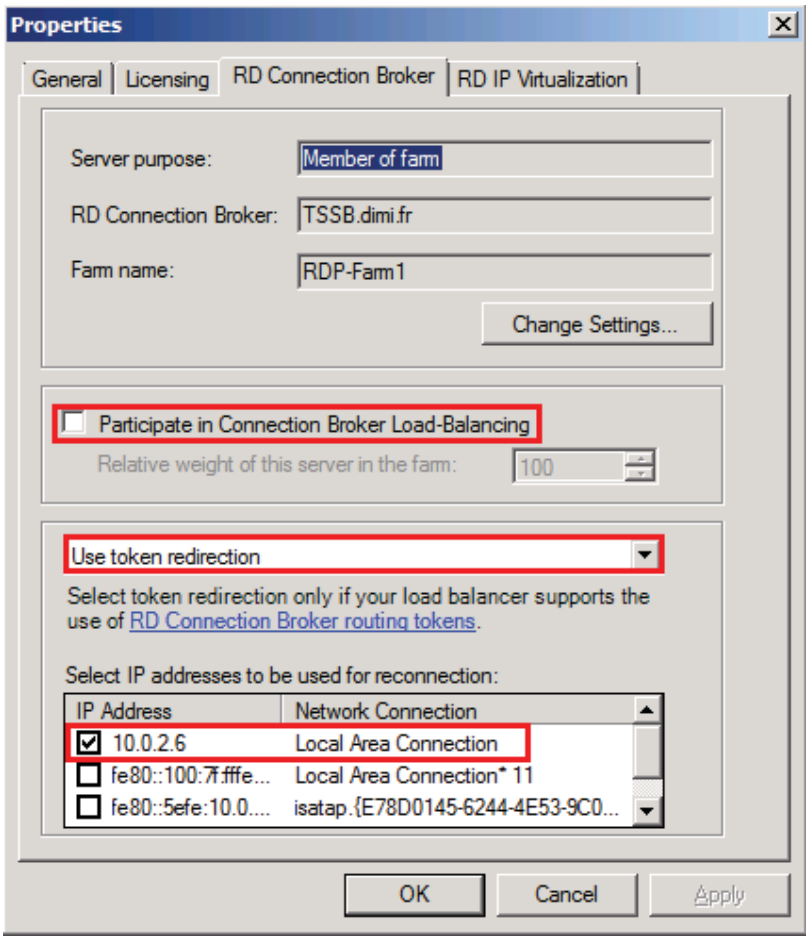
Figure 1: Microsoft TS with RDC access deployment

Microsoft TS configuration with the AX Series load balancer

Note: To download a step-by-step guide for Microsoft TS, visit: http://technet.microsoft.com/en-us/library/cc772418%28WS.10%29.aspx

As explained in the Microsoft guide, to deploy with load balancers, configure the following Remote Desktop Connection Broker settings on each TS. Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration - Edit Settings / RD Connection Broker. Use the following settings:

- Deselect **Participate in Connection Broker Load-balancing**. (Load balancing is performed by the AX device.)
- Select **Use token redirection**. (When an end user closes their RDP connection without logging out and then reconnects, the end-user does not reconnect directly to the TS. Instead, they provide the TS IP address information in a routing token used by the load balancer to know where to redirect the end-user.)
- Select the IP address of the TS provided in the token. (This must be the Terminal Server IP address defined on the AX device.)



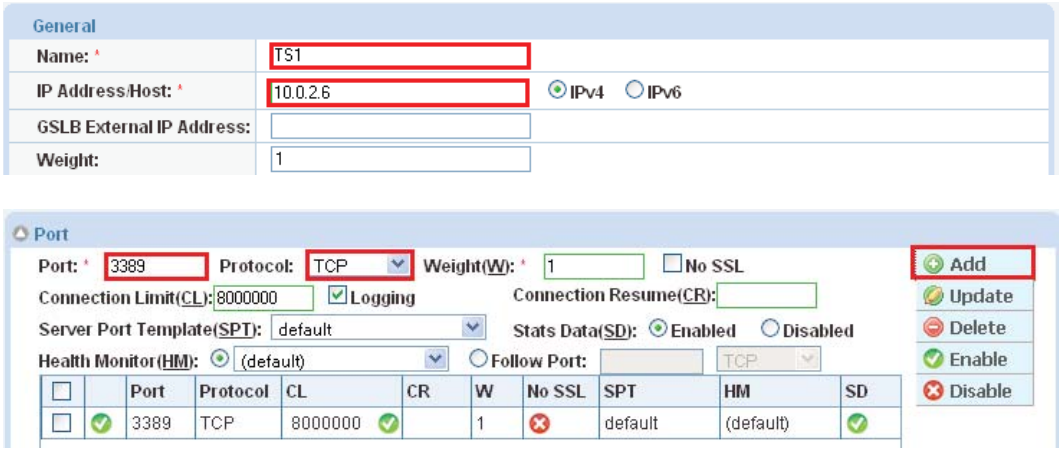
AX configuration

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

AX configuration steps:

1. Create a real server for each TS. Enter the TS name and IP address, and add TCP port 3389.

   - Via Web GUI: Config Mode > Service > SLB > Server

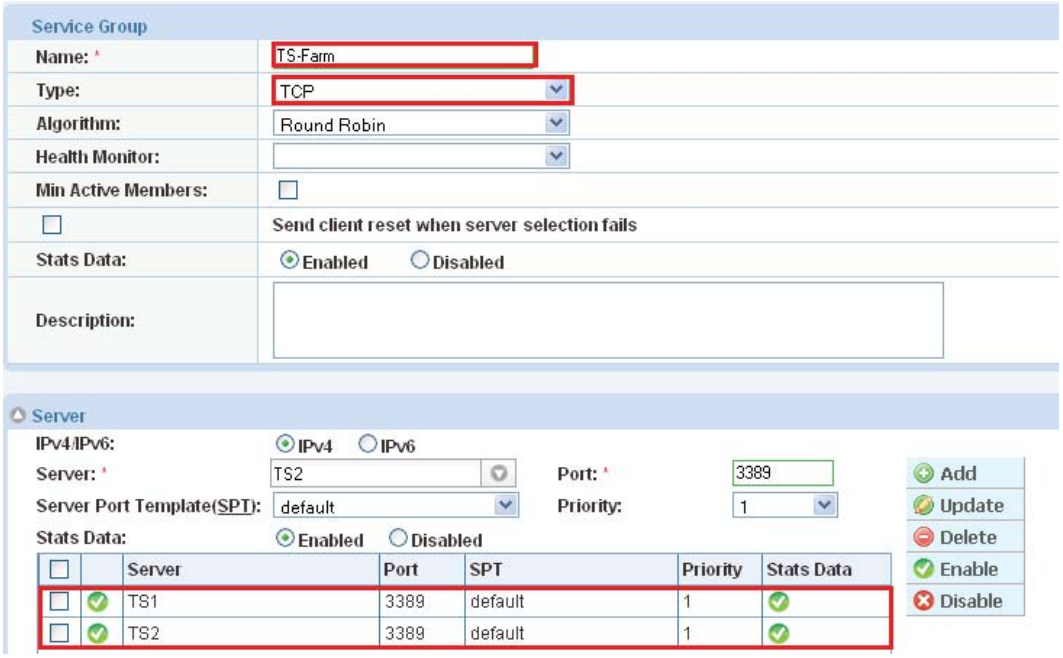


   - Via CLI:

```
AX(config)#slb server TS1 10.0.2.6
AX(config-real server)#port 3389 tcp
```

2. Create the service group (TS farm).
   Enter a name for the service group, and select **TCP** from the **Type** drop-down list. Assign each TS to the service group.

◦ Via Web GUI: Config Mode > Service > SLB > Service Group



◦ Via CLI:

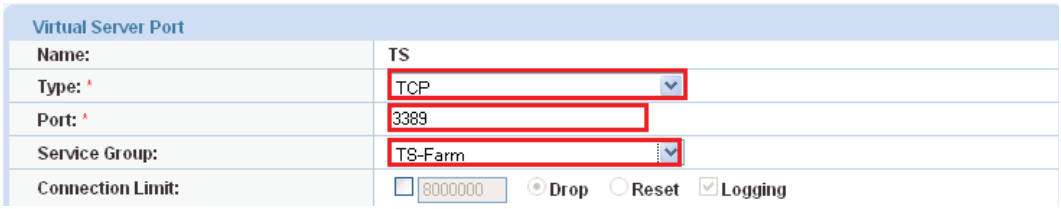
```
AX(config)#slb service-group TS-Farm tcp
AX(config-slb svc group)#member TS1:3389
AX(config-slb svc group)#member TS2:3389
```

3. Create the virtual IP address (VIP), which is the IP address that clients will access.
   a. Enter a name for the VIP, and enter the IP address.
   ◦ Via Web GUI: Config Mode > Service > SLB > Virtual Server

◦ Via CLI: `AX(config)#slb virtual-server TS 62.52.24.31`

   b. Add the TCP port and select the service group.

- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

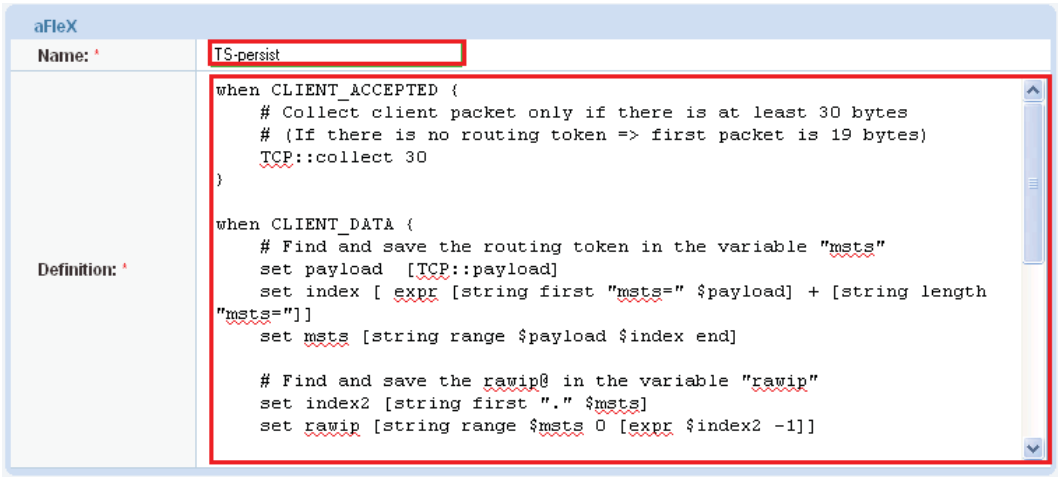


- Via CLI:
```
AX(config-slb vserver)#port 3389 tcp
AX2(config-slb vserver-vport)#service-group TS-Farm
```

4. Create an aFleX policy, to define the TS persistence rule:

```
when CLIENT_ACCEPTED {
  # Collect client packet only if there is at least 30 bytes
  # (If there is no routing token => first packet is 19 bytes)
  TCP::collect 30
}

when CLIENT_DATA {
  # Find and save the routing token in the variable "msts"
  set payload [TCP::payload]
  set index [ expr [string first "msts=" $payload] + [string length
"msts="]]

  #only if there is a routing token
  if {$index ne 4} {
    set msts [string range $payload $index end]

    # Find and save the rawip@ in the variable "rawip"
    set index2 [string first "." $msts]
    set rawip [string range $msts 0 [expr $index2 -1]]

    # Find and save the raw tcp port in the variable "rawport"
    set msts2 [string range $msts [expr $index2 + 1] end]
    set index3 [string first "." $msts2]
    set rawport [string range $msts2 0 [expr $index3 - 1]]
    # Convert and save the real tcp port in the variable "port"
    set port [ntohs [format "%d" $rawport]]
    # Convert and save the real ip@ in the variable "ipaddr"
    set bin [binary format i $rawip]
    binary scan $bin cccc a b c d
    set a [expr { $a & 0xff }]
    set b [expr { $b & 0xff }]
    set c [expr { $c & 0xff }]
    set d [expr { $d & 0xff }]
    set ipaddr "$a.$b.$c.$d"
    node $ipaddr $port
    # print the node
    # log "node= $ipaddr $port"
  }
}
```

- Via Web GUI: Config Mode > Service > aFleX



- Via CLI: `AX(config)#import aflex TS-persist tftp://172.31.31.12/TS-persist`

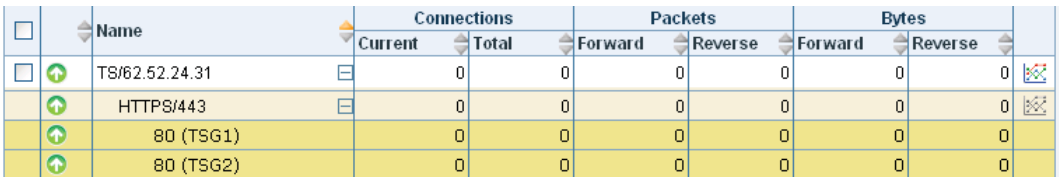
5. Assign the aFleX policy to the virtual server.
   - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

   - Via CLI:
```
AX(config)#slb virtual-server TS 62.52.24.31
AX(config-slb vserver)#port 3389 tcp
AX(config-slb vserver-vport)#aflex TS-persist
```

AX VIP status

Display the status of the VIP and its members:

- Via Web GUI: Config Mode > Service > SLB > Virtual Server



Name	Connections		Packets		Bytes	
	Current	Total	Forward	Reverse	Forward	Reverse
TS/62.52.24.31	0	0	0	0	0	0
HTTPS/443	0	0	0	0	0	0
80 (TSG1)	0	0	0	0	0	0
80 (TSG2)	0	0	0	0	0	0

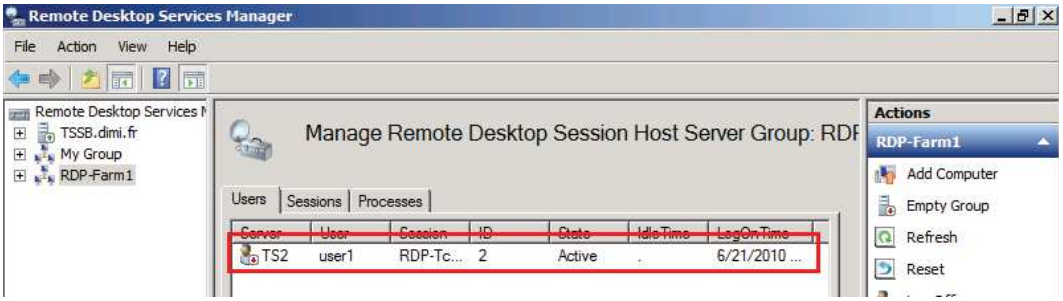
- Via CLI:
```
AX#show slb virtual-server TS
AX#show slb service-group TSG-Farm
AX#show slb server [TSG1 | TSG2]
```

AX deployment validation

To validate the AX deployment:

1. Verify that clients can access the TS farm using RDP access via the VIP:
   - Launch RDP (mstsc.exe) and connect to the VIP.

   - Validate that the client has access to a TS.
   - Administrative Tools > Remote Desktop Services > Remote Desktop Services Manager, and go to the TS group.



2. Verify persistence. Have one client close its RDP session (without logging out from the TS), and reconnect. The AX device should send the new connection to the same TS.

- Open an application (for instance, “Notepad”) and close the RDP session without logging out from the TS.

- Establish a new RDP connection (from the same PC or another one) and log in with the same user. The new RDP connection is on the same server and the application is still there.

AX deployment for Windows TS with RDC with TSG access

Windows 2008 enhanced its TS with a new role: Gateway. TS Gateway provides RDP connection over HTTPS. The Gateway role enables remote end-users to access the TS farm, even when the RDP protocol is blocked by a firewall and only HTTP/HTTPS is authorized.

The AX device fully supports Microsoft TS Gateway and allows:

- Large TS Gateway farms
- Granular TS Gateway loadbalancing and availability options
- TS Gateways in private networks (which are not directly reachable from outside)
- Optional SSL offload on TS Gateways

Note: The same AX device can be used for TS with RDS (described in the previous section) and TS with RDC with TSG.

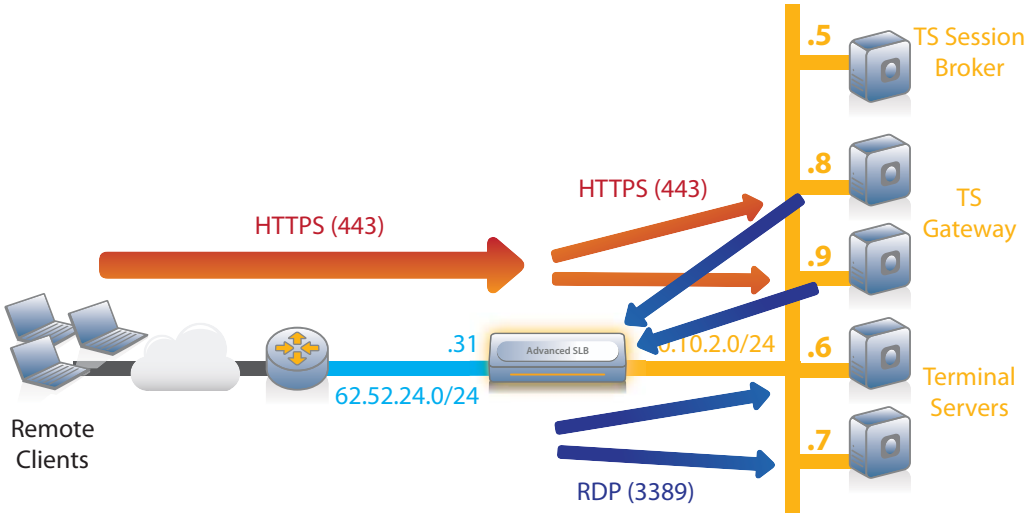
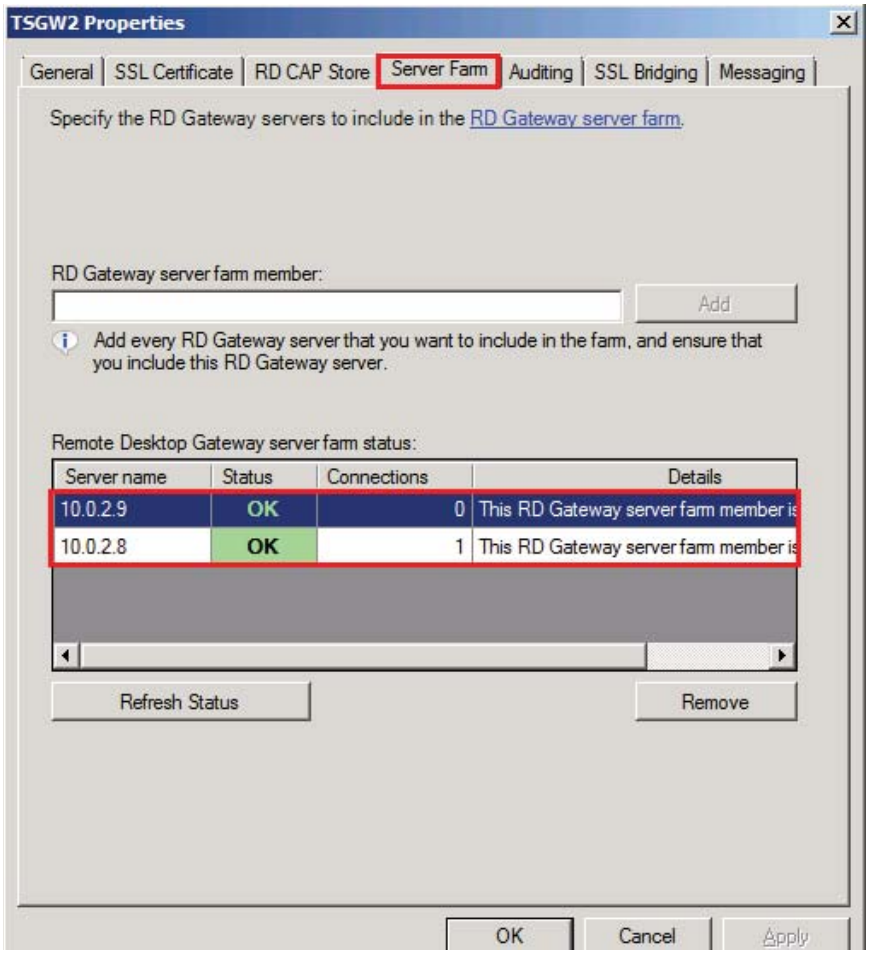


Figure 2: Microsoft TS with RDC with TSG access deployment

Microsoft TS Gateway configuration with load balancers such as AX

Note: To download a step-by-step guide for Microsoft TS Gateway, visit: http://technet.microsoft.com/en-us/library/cc771530%28WS.10%29.aspx

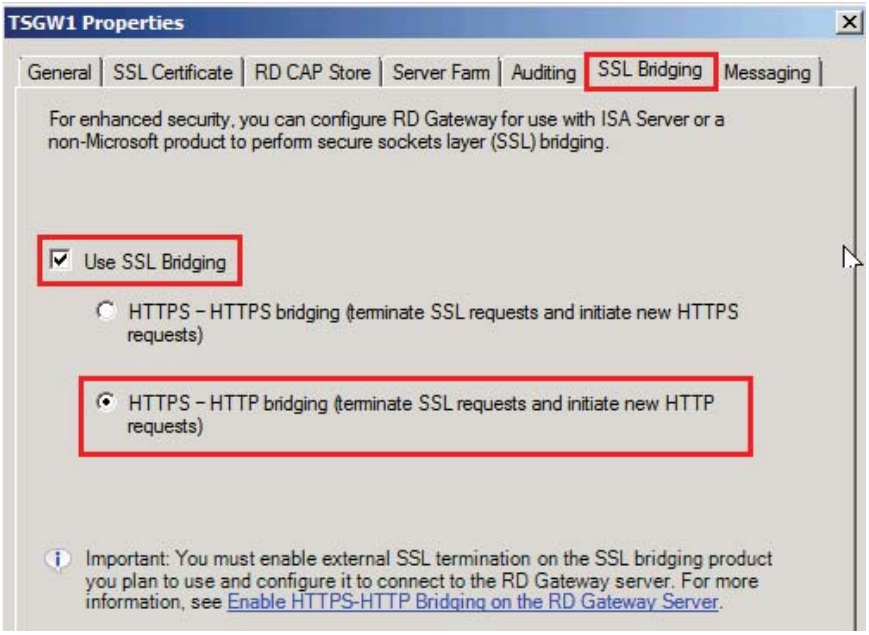
As explained in the Microsoft guide, to deploy with load balancers, configure the following settings on each TS Gateway. (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager – Edit Properties / Server Farm.)



When deployed with load balancers configured with no TS Gateway SSL offload, use the same server certificate for the following on all TS Gateways:

- IIS (Navigate to Administrative Tools > IIS - Select Server > Sites > Default Web Site - Edit Site Bindings.)
- Terminal Service Gateway (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager – Edit Properties / SSL Certificate) on all TS Gateways.

When deployed with load balancers that are configured with TS Gateway SSL offload, configure HTTPS-HTTP bridging on each TS Gateway. (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager – Edit Properties / SSL Bridging.)



AX configuration

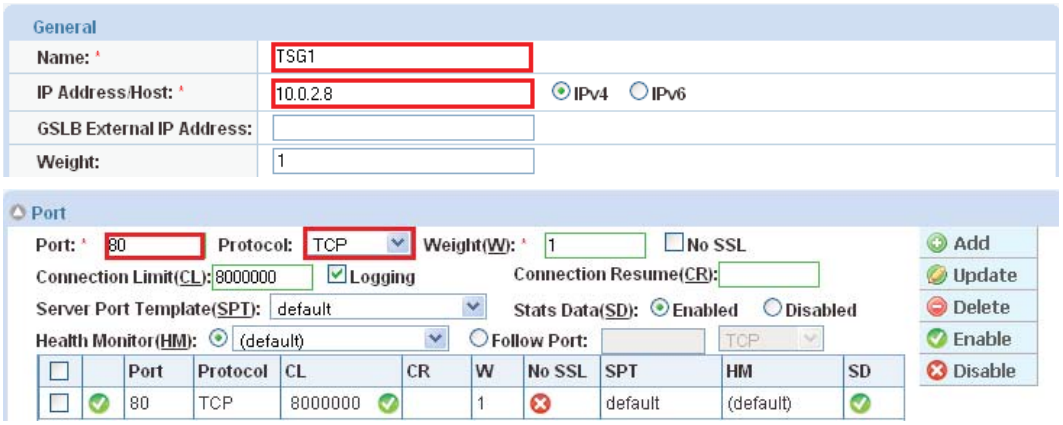
The steps below detail the AX configuration for TS Gateway with SSL offload. If you do not want to offload SSL on TS Gateway, see the "No SSL Offload Note" in each step.

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

AX configuration steps:

1. Create a real server for each TS Gateway. Enter the TS name and IP address, and add TCP port 80.
   *No SSL Offload Note: Replace port **80** with **443**.*

- Via Web GUI: Config Mode > Service > SLB > Server



- Via CLI:

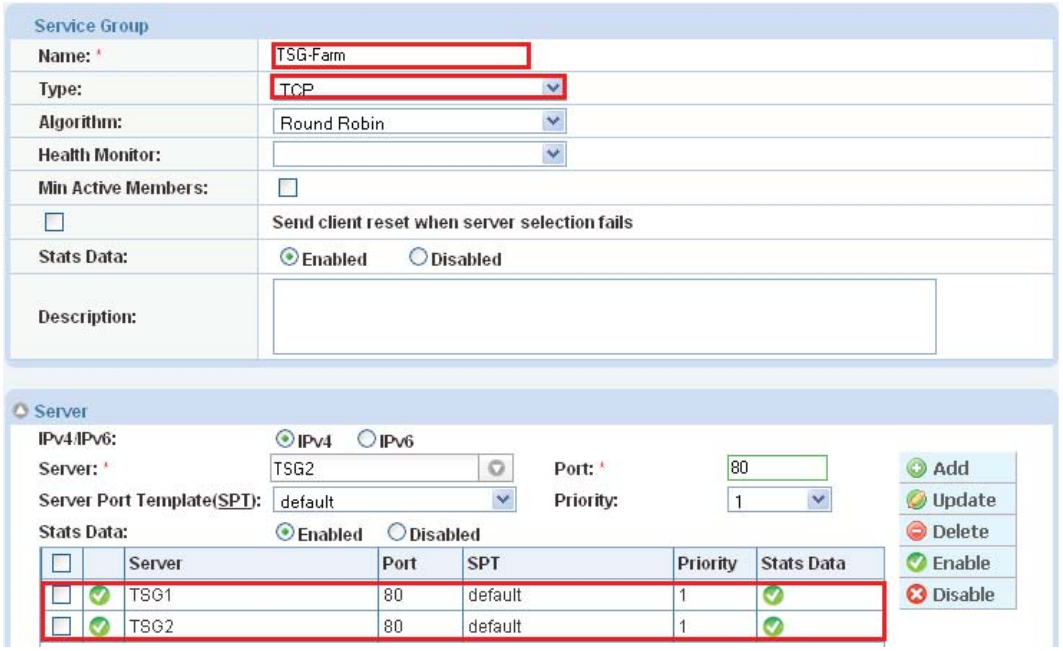
```
AX(config)#slb server TSG1 10.0.2.8
AX(config-real server)#port 80 tcp
```

2. Create a service group for the TS Gateway farm.

   Enter a name for the service group, and select **TCP** from the **Type** drop-down list. Assign each TS Gateway to the service group.

   *No SSL Offload Note: Replace port **80** with **443**.*

   - Via Web GUI: Config Mode > Service > SLB > Service Group



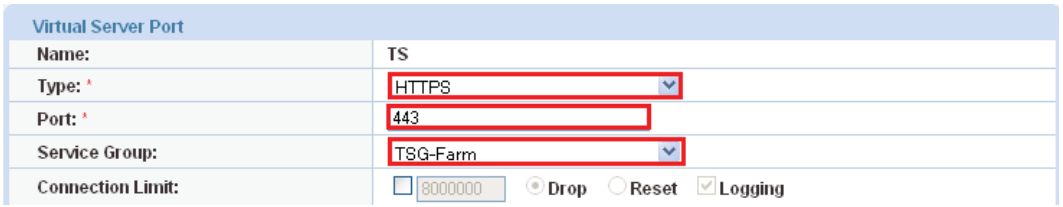
- Via CLI:

```
AX(config)#slb service-group TSG-Farm tcp
AX(config-slb svc group)#member TSG1:80
AX(config-slb svc group)#member TSG2:80
```

3. Create the virtual IP address (VIP), which is the IP address that clients will access.
   *No SSL Offload Note: In step b, replace port type **HTTPS** with **TCP**.*
   a. Enter a name for the VIP, and enter the IP address.
   ◦ Via Web GUI: Config Mode > Service > SLB > Virtual Server

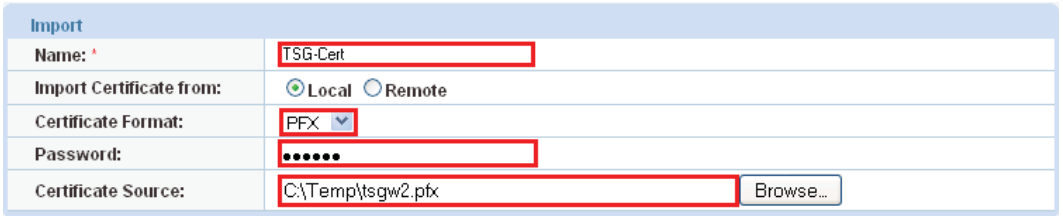
   ◦ Via CLI: `AX(config)# slb virtual-server TS 62.52.24.31`

   b. Add the HTTPS port and select the service group.
   ◦ Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



   ◦ Via CLI:
```
AX(config-slb vserver)#port 443 https
AX2(config-slb vserver-vport)#service-group TSG-Farm
```

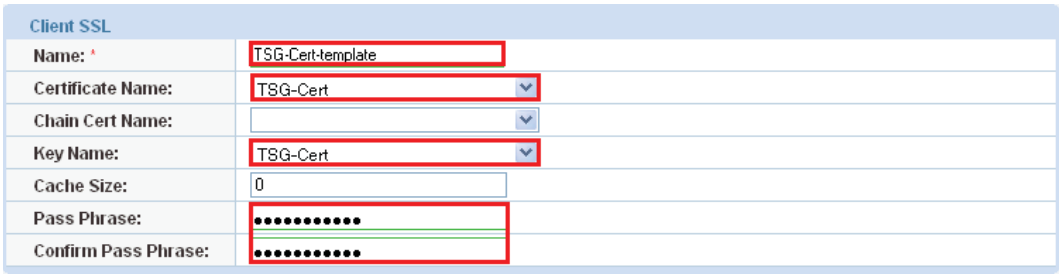
4. Import the TS Gateway certificate onto the AX device, and add it to a client-SSL template:
   No SSL Offload Note: Skip this step.
   a. Enter a name for the certificate, select the import method (**Local** or **Remote**), and select the format. Enter or select download settings. (These depend on whether you select **Local** or **Remote**.)
   ◦ Via Web GUI: Config Mode > Service > SSL Management > Certificate



   ◦ Via CLI: `AX(config)#slb ssl-load certificate TSG-Cert type pfx password a10 tftp://10.0.1.10/tsgw2.pfx`

b. Create a client-SSL template. Enter a name for the template, select the certificate and key files, and enter the passphrase.

- Via Web GUI: Config Mode > Service > Template > SSL > Client SSL

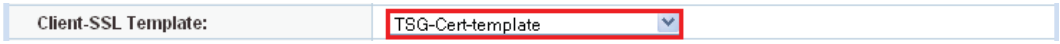


- Via CLI:

```
AX(config)#slb template client-ssl TSG-Cert-template
AX(config-client ssl)#cert TSG-Cert
AX(config-client ssl)#key TSG-Cert passphrase a10
```

5. Assign the client-SSL template to the virtual server port.
No SSL Offload Note: Skip this step.

- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



- Via CLI:

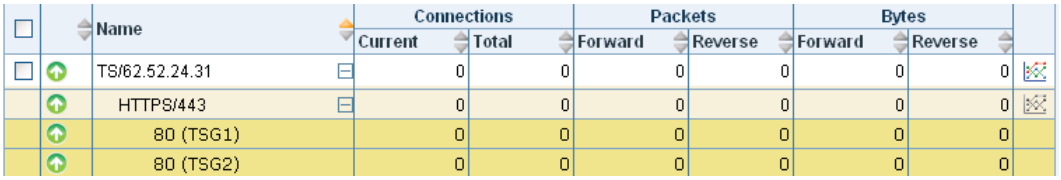
```
AX(config)#slb virtual-server TS 62.52.24.31
AX(config-slb vserver)#port 443 https
AX(config-slb vserver-vport)#template client-ssl TSG-Cert-tem-
plate
```

Note: TS Gateways do not need persistence. Each TS Gateway is aware of all user connections. When an end-user closes their RDP connection without logging out, and then reconnects, the connection may be load balanced to another TS Gateway. The TS Gateway simply forwards the end-user traffic to the correct TS Gateway.

AX VIP status

Display the status of the VIP and its members:

1. Via Web GUI: Config Mode > Service > SLB > Virtual Server



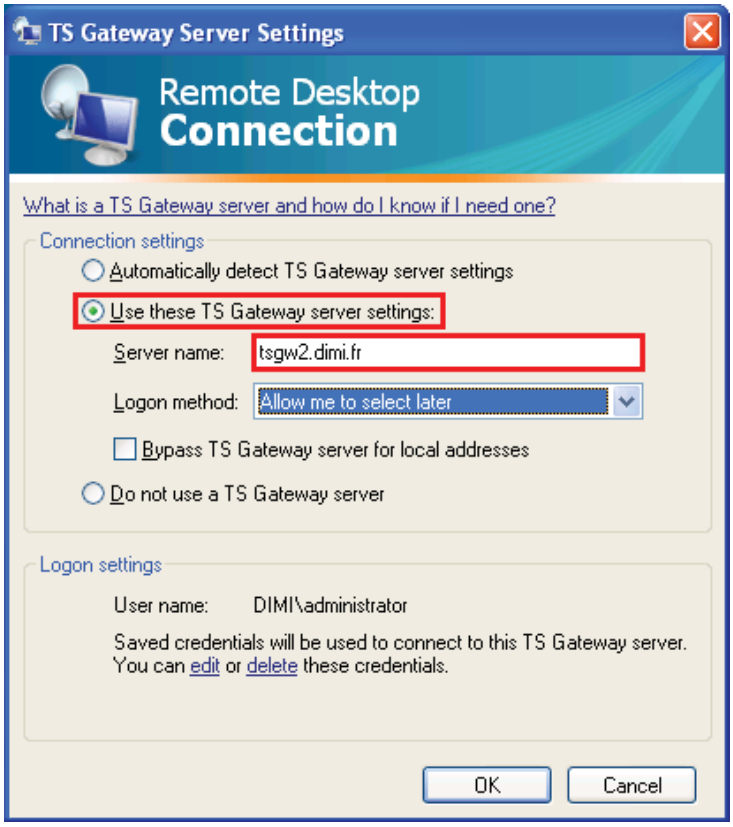
	Name	Connections		Packets		Bytes		
		Current	Total	Forward	Reverse	Forward	Reverse	
	TS/62.52.24.31	0	0	0	0	0	0	
	HTTPS/443	0	0	0	0	0	0	
	80 (TSG1)	0	0	0	0	0	0	
	80 (TSG2)	0	0	0	0	0	0	

2. Via CLI:
```
AX#show slb virtual-server TS
AX#show slb service-group TSG-Farm
AX#show slb server [TSG1 | TSG2]
```

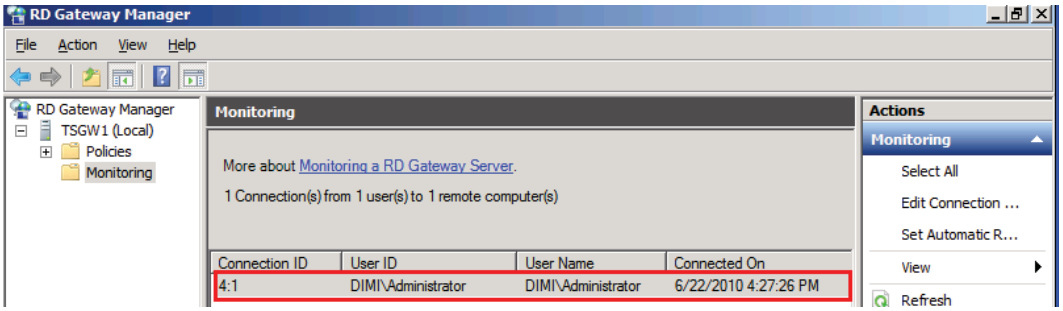
AX deployment validation

To validate the AX deployment:

1. Verify that clients can access the Terminal Servers using RDP with TSG access via the VIP:
   - Launch RDP (mstsc.exe) and connect to the TS with the TSG option configured. (Navigate to Options – Advanced > Settings.)



   - Validate that the client has access to a TS.
   - On the TS Gateway, validate that the TS Gateway is aware of the client connection. (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager + Go to Monitoring.)



AX deployment for Windows TS with Web access

Windows 2008 enhanced TS with a new role: Web Access. TS Web Access provides web access to distributed applications on TS.

End customers access the web portal that provides the list of distributed applications on TS. Then they connect to these applications via RDP to the TS.

The AX device fully supports Microsoft TS Gateway with Web access and allows:

- Large TS Gateway farms
- Granular TS Gateway load balancing and availability options
- TS Gateways in private networks (not directly reachable from outside)
- (optional) SSL offload on TS Gateways

Note: The same AX device can be used for TS with RDS and TS with RDC with TSG.

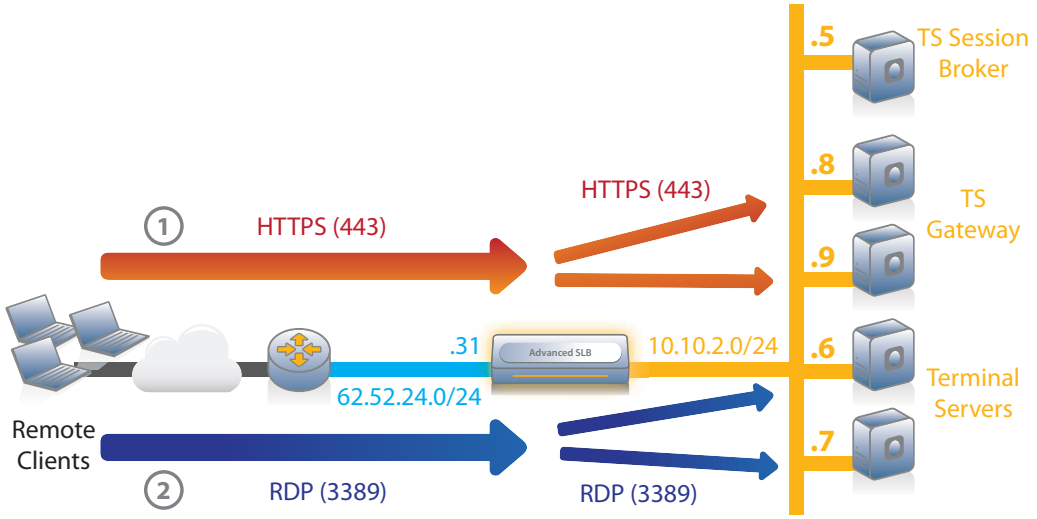


Figure 3: Microsoft TS with Web access deployment

Microsoft TS Gateway configuration with load balancers such as AX

Note: To download a step-by-step guide for Microsoft TS Gateway, visit: http://technet.microsoft.com/en-us/library/cc771354(WS.10).aspx

TS Web Access does not need any specific configuration when deployed with load balancers.

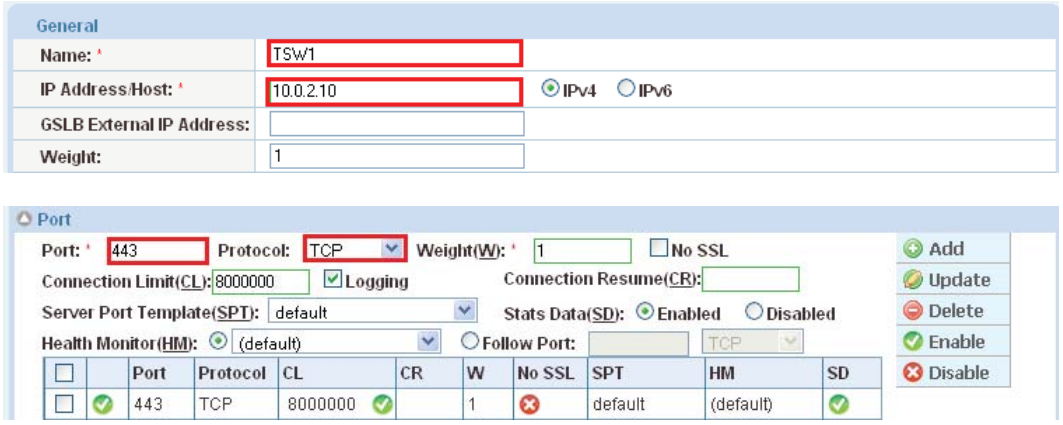
AX configuration

The steps below detail AX configuration for TS Web Access.

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

AX configuration steps:

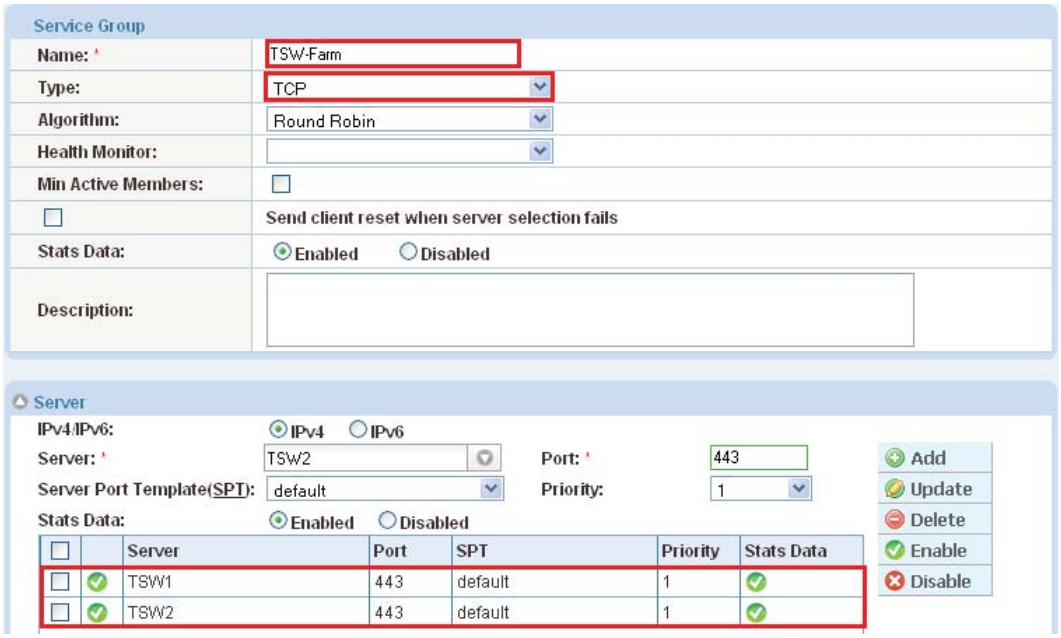
1. Create a real server for each TS Gateway. Enter the TS name and IP address, and add TCP port 443.
   - Via Web GUI: Config Mode > Service > SLB > Server



   - Via CLI:

```
AX(config)#slb server TSW1 10.0.2.10
AX(config-real server)#port 443 tcp
```

2. Create a service group for the TS Gateway farm.
   - Via Web GUI: Config Mode > Service > SLB > Service Group



   - Via CLI:
```
AX(config)#slb service-group TSW-Farm tcp
AX(config-slb svc group)#member TSW1:443
AX(config-slb svc group)#member TSW2:443
```

3. Create the virtual IP address (VIP), which is the IP address that clients will access.
   a. Enter a name for the VIP, and enter the IP address.
   - Via Web GUI: Config Mode > Service > SLB > Virtual Server

   - Via CLI: `AX(config)#slb virtual-server TS 62.52.24.31`

b. Add the HTTPS port and select the service group.

- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

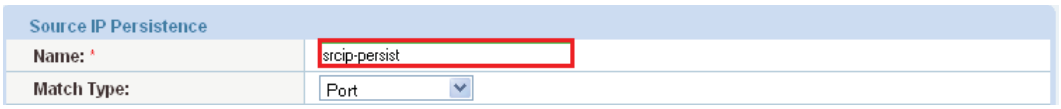
- Via CLI:

```
AX(config-slb vserver)#port 443 tcp
AX2(config-slb vserver-vport)#service-group TSW-Farm
```

4. Configure persistence for TS Web access:

a. Create a source-IP persistence template. Only a name is required.

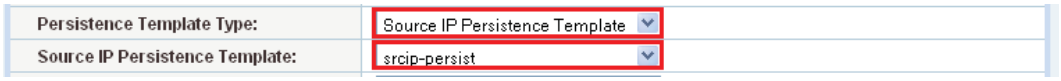
- Via Web GUI: Config Mode > Service > Template > Persistent > Source IP Persistence



- Via CLI: `AX(config)#slb template persist source-ip srcip-persist`

b. Assign the source-IP persistence template to the virtual server.

- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



- Via CLI:

```
AX(config)#slb virtual-server TS 62.52.24.31
AX(config-slb vserver)#port 443 tcp
AX(config-slb vserver-vport)#template persist source-ip srcip-
persist
```

AX VIP status

Display the status of the VIP and its members:

1. Via Web GUI: Config Mode > Service > SLB > Virtual Server

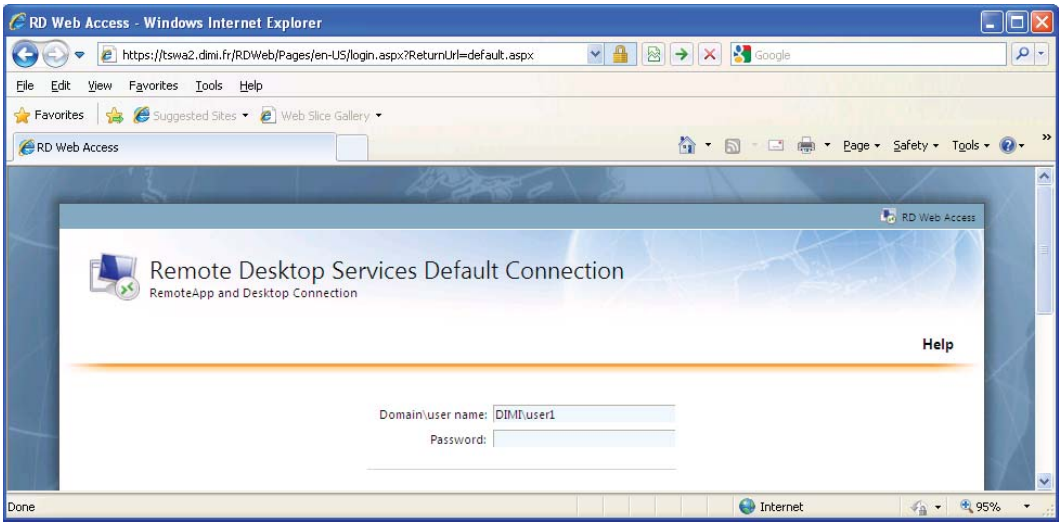
		Name	Connections		Packets		Bytes		
			Current	Total	Forward	Reverse	Forward	Reverse	
☐		TS/62.52.24.31	0	0	0	0	0	0	
		TCP/443	0	0	0	0	0	0	
		443 (TSW1)	0	0	0	0	0	0	
		443 (TSW2)	0	0	0	0	0	0	

2. Via CLI:
```
AX#show slb virtual-server TS
AX#show slb service-group TSW-Farm
AX#show slb server [TSW1 | TSW2]
```

AX deployment validation

To validate the AX deployment:

1. Verify that clients can access the Terminal Servers using Web access via the VIP:
   - Launch Internet Explorer and connect to the TS Web Access servers.



   - Validate that the client has access to the distributed applications.

Summary and Conclusion

The AX Series Advanced Traffic Manager provides Windows Server 2008 Terminal Services load balancing with:

- High availability
- High scalability
- High flexibility
- High performance
- High security

For more information about AX Series products, refer to:
http://a10networks.com/products/axseries.php
http://a10networks.com/resources/solutionsheets.php
http://a10networks.com/resources/casestudies.php

About A10 Networks

A10 Networks was founded in 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations accelerate, optimize and secure their applications. A10 Networks is headquartered in Silicon Valley with offices in the United States, Europe, Japan, China, Korea and Taiwan. For more information, visit www.a10networks.com.

Performance by Design

To learn more about the AX Series Advanced Traffic Manager and how to improve application performance up to 8 times faster while enhancing reliability and security, visit A10 Networks' website at:
www.a10networks.com
Or call and talk to an A10 sales representative:

Corporate Headquarters

A10 Networks, Inc.
2309 Bering Drive
San Jose, CA 95131
Tel: +1 408 325-8668
Fax: +1 408 325-8666

North America Sales:

+1 888 A10-6363
+1 408 325-8616

Europe, Middle East & Africa Sales:

+31 70 799-9143

Asia Pacific Sales:

China, Beijing Office:
+86 10 8515-0698

China, Shanghai Office:
+86 21 6137-7850

Japan Sales:
+81-3-3291-0091

Korea Office:
+82-2-6007-2150
+82-2-6007-2151

Taiwan Office:
+886-2-2657-3198